Local indistinguishability and LOCC monotones

Michał Horodecki[1], Aditi Sen(De)[2], Ujjwal Sen[3] and Karol Horodecki[4]

Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland

Abstract

We provide a method for checking indistinguishability of a set of orthogonal states by local operations and classical communication (LOCC). It bases on the principle of nonincreasing of entanglement under LOCC. This method originates from the one introduced by Ghosh *et al.* (Phys. Rev. Lett. **87**, 5807 (2001) (quant-ph/0106148)), though we deal with *pure* states. We apply it to show that an arbitrary complete orthogonal basis of an $m \otimes n$ system is indistinguishable if it contains at least one entangled state. We also show that probabilistic distinguishing is possible for full basis if and only if all vectors are product.

Orthogonal quantum state vectors can always be distinguished if there are no restrictions to measurements that one can perform. If the vectors are states of a system consisting of two distant subsystems, then there can be natural restrictions for the measurements that can be done. In particular, if Alice and Bob (the parties holding the subsystems) cannot communicate quantum information, their possibilities significantly decrease [1]. Intuitively one feels that in such a case, there will be a problem with distinguishing entangled states, while product ones should remain distinguishable. The first result in this area was rather surprising: in Ref. [3] the authors exhibited a set of pure *product* states, that cannot be distinguished with certainty by local operations and classical communications (LOCC). Another counterintuitive result was obtained in Ref. [4]: *any* two orthogonal states can be distinguished from each other by LOCC, irrespective of how entangled they are. There is therefore a general question: which sets of states are distinguishable?

To find that a given set *is* distinguishable, one usually needs to build suitable protocol. To show that the states are *not* distinguishable one can try to eliminate all possible measurements as in [5]. Another way is to employ somehow the theory of entanglement [2, 6, 7, 8]. A typical statement proving such indistinguishability would be then: Alice and Bob cannot distinguish the states, as they would increase entanglement otherwise (which is impossible by LOCC). The advantage of the latter method is that it allows to estimate the entanglement resources needed to distinguish the states, that are non-distinguishable by LOCC.

In Ref. [9] this approach was first used to check distinguishability between two mixed states (we will call it TDL method). Another powerful method based on entanglement was recently designed in Ref. [10] (we will call it GKRSS method). In this paper we introduce another method, closely related to the latter one, and connected also with the TDL method. Our approach provides a strong tool for investigation of distinguishability of sets pure states, becasue it bases on deciding whether some pure state can be transformed into some other pure states by LOCC, the latter issue being completely solved in a series of papers on entanglement monotones and entanglement manipulations with pure states [7, 11, 12, 13]. Using it, we show that any full basis of two systems is not distinguishable, if at least one of vectors is entangled [14]. For $2 \otimes n$ system it is then also "only if", as product bases are distinguishable in this case [15]. Our result applies also to probabilistic distinguishability, so that in conjunction with the result of [17] we obtain that a full basis is probabilistically distinguishable if and only if all vectors are product.

Let us first note that the application of entanglement theory to this problem is not immediate. Imagine, that we want to distinguish between the four Bell states given by

$$\begin{aligned} |B_1\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |B_2\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |B_3\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |B_4\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned}$$

[1] fizmh@univ.gda.pl
[2] aditi@iftia6.univ.gda.pl
[3] ujjwal@univ.gda.pl
[4] khorodec@manta.univ.gda.pl

If we were able to apply by LOCC just the von Neumann measurement, then we could obviously create entanglement. Namely, if Alice and Bob start with any initial state (hence also possibly a disentangled one), after the von Neumann measurement, it collapses into one of Bell states. This is of course impossible. We cannot however conclude at this moment, that they are indistinguishable. The clue is that we could distinguish between them, while destroying them during the process. Thus Alice and Bob would get to know what state they shared, but the potential entanglement would be destroyed. This is actually the case in the Walgate *et al.* protocol [4], where one distinugishes between two (possibly) entangled states.

To employ entanglement theory in the distinguishability question, a more clever method should be applied. The general hint is to apply the measurement to some larger system. This concept is a basis for the TDL and GKRSS methods. In the first one [9] the authors considered a state of four systems A, B, C, D:

$$\psi = \psi_{AB} \otimes \psi_{CD}$$

where ψ_{AB} and ψ_{CD} are maximally entangled states. Then the measurement is applied to the AB part (cf. [17]). If the state after measurement is entangled, then one concludes that the measurement cannot be done by use of LOCC.

The GKRSS method [10] is the following. Given the set of states $\{\psi_i^{AB}\}_{i=1}^k$ to be distinguished, one builds a mixed state

$$\varrho = \frac{1}{k}\sum_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i| \tag{1}$$

where ϕ_i are some entangled states of the CD system (more generally one could put some probabilities p_i instead of $1/k$). Now if Alice(A) and Bob(B) are able to distinguish between the states ψ_i they can tell the result of their measurement to Claire(C) and Danny(D), who will then share states ϕ_i with probability $1/k$. One now compares the initial entanglement $E(\varrho)$ measured across the AC:BD cut and the final one given by $(1/k)\sum_i E(\phi_i)$ according to any chosen entanglement measure E. If the states ψ_i are distinguishable by LOCC, then the final entanglement cannot be greater than the initial one; otherwise one could increase entanglement by LOCC [18]. Thus, if we have

$$E(\varrho) < \frac{1}{k}\sum_i E(\phi_i) \tag{2}$$

then the states ψ_i are not distinguishable by LOCC. In Refs. [10, 20] distillable entanglement was used as E.

Let us now exhibit the method of the present paper. It is a modification of the GKRSS method. Namely instead of classical correlations between AB and CD we will use quantum correlations. Consequently mixture (2) is replaced by the *superposition*

$$\psi_{ABCD} = \sum_i \sqrt{p_i}\,|\psi_i^{AB}\rangle\,|\phi_i^{CD}\rangle \tag{3}$$

The states ϕ_i will be used here essentially to *detect* as to whether a set of states are locally indistinguishable and as such we shall henceforth call them "detectors". At a first glance it seems that this approach should fail, because the pure state is unlikely to have small entanglement. In [10] where mixtures are used, the possibility for the initial state ϱ_{ABCD} to be separable in the AC:BD cut was much larger, as mixed states are less coherent than pure ones; for a pure state to be separable, it has to be product, while for mixed states, the very mixedness can decrease entanglement, or even produce separability [21]. Let us however exhibit the following example. Suppose that Alice and Bob are to distinguish between the Bell states $|B_i\rangle$. As detectors, we take the same states (as in [10]). Our pure state is thus

$$|\psi\rangle_{ABCD} = \frac{1}{2}\sum_{i=1}^{4} |B_i\rangle_{AB}\,|B_i\rangle_{CD}$$

One can see that this state can be written as

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AC}\,\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{BD}$$

So it turns out that it is *product* in AC:BD cut, so that our method will work. Assuming now the four Bell states to be locally distinguishable immediately would imply that the state $|\psi\rangle$ is entangled in the AC:BD cut which is the desired contradiction. This result was obtained in [10] and their mixed state $\varrho_{ABCD} = \frac{1}{4}\sum_i |B_i\rangle\langle B_i| \otimes |B_i\rangle\langle B_i|$ turned out to be separable in AC:BD (see also [22]). Here we have a pure state which is product. Note that in this particular example, our method, even though originating from the GKRSS approach, coincides with the TDL method.

The advantage of our approach over the GKRSS method is that for mixed states, it is usually hard to check the relation (2) for different entanglement measures. Indeed, for mixed states it is difficult to evaluate the known entanglement measures. In our case we have pure states on both sides of the inequality, for which the set of all needed measures is known [7, 12]. Even more: Jonathan and Plenio [13], generalizing the Nielsen result [11], have obtained a necessary and sufficient condition for the transformation from a pure state ϕ to an ensemble of pure states $\{p_i, \phi_i\}$. The condition is efficiently computable. Namely, let λ and λ_i be vectors of the Schmidt coefficients of ϕ and ϕ_i respectively. Then the LOCC transition $\phi \to \{p_i, \phi_i\}$ is possible if and only if the vector $\sum_i p_i\lambda_i$ majorizes λ [23]. To summarise, our method consists of the following steps

(1) Given the states $\{\psi_i^{AB}\}_{i=1}^k$ to be distinguished, choose k detectors ϕ_i^{CD} and probabilities p_i.

(2) Applying the Jonathan-Plenio criterion, check if the transition $\psi_{ABCD} \to \{p_i, \phi_i^{CD}\}$ is possible by LOCC (in AC:BD cut) where ψ_{ABCD} is of the form (3).

The item (1) can be formulated more generally in the following way:

(1a) Choose ψ_{ABCD} such that its reduction ϱ_{AB} has the support spanned by ψ_i^{AB}'s.

(1b) Determine detectors ϕ_i^{CD} by writing ψ_{ABCD} by means of ψ_i^{AB}.

Now we will apply our method to obtain the following proposition, where in fact we do not need an explicit use of the Jonathan-Plenio criterion.

Proposition. Let ψ_i^{AB} be a full orthogonal basis of an $m \otimes n$ system. Then we have: (1) If at least one of the vectors is entangled (see [14]), the set cannot be perfectly distinguished by LOCC (2) The set cannot be probabilistically distinguished if and only if all vectors are product.

Remark. Note that we will not have "if and only if" for item (1) because there are orthogonal product bases that cannot be distinguished [3]. However it would also be "only if" in $2 \otimes n$, as all product bases are locally distinguishable there [15].

Proof. Consider the four party state

$$|\psi\rangle_{ABCD} = \left(\frac{1}{\sqrt{m}}\sum_{i=1}^{m}|ii\rangle_{AC}\right)\left(\frac{1}{\sqrt{n}}\sum_{j=1}^{n}|jj\rangle_{BD}\right)$$

shared between Alice, Bob, Claire and Danny, which is product across the AC:BD cut. Note that Alice and Claire are sharing m -dimensional systems each while Bob and Danny are sharing n -dimensional systems each. Written in AB:CD, this state takes the form

$$\frac{1}{\sqrt{mn}}\sum_{k=1}^{mn}|k\rangle_{AB}|k\rangle_{CD}$$

However we know that such a state is $U \otimes U^*$ invariant where U is an arbitrary unitary operator on the mn-dimensional Hilbert space (with the tensor product separating AB from CD) and where the complex conjugation is taken in the computational basis (see e.g. [24]). We would choose our U as indicated below.

Let $\{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_{mn}\rangle\}$ be a set of mn orthonormal states of an $m \otimes n$ system. We choose our U such that $U|k\rangle = |\psi_k\rangle$ for all $k = 1, 2, ..., mn$. We now use the $U \otimes U^*$ invariance of the state $|\phi\rangle$ in the AB:CD cut and write it as

$$\frac{1}{\sqrt{mn}}\sum_{k=1}^{mn}|\psi_k\rangle_{AB}|\psi_k\rangle_{CD}^*$$

where the complex conjugation is again in the computational basis.

Therefore if Alice and Bob are able to locally distinguish between the $|\psi_k\rangle$s, they could ring up Claire and Danny to tell which state they share, resulting in the creation of the corresponding correlated state $|\psi_k\rangle^*$ between Claire and Danny.

Now if at least one among the $|\psi_k\rangle$s is entangled, an assumption of local distinguishability of the $|\psi_k\rangle$s would imply that the state $|\psi\rangle$ has a nonzero amount of entanglement in the AC:BD cut [25]. But this is forbidden as $|\psi\rangle$ is product in the AC:BD cut.

Note that the above reasoning goes through irrespective of whether the local distinguishability protocol for the $|\psi_k\rangle$s is deterministic or probabilistic. This proves that an arbitrary complete set of orthogonal states of any bipartite system is locally indistinguishable (deterministically as well as probabilistically) if at least one of vectors is entangled. (Note that for the desired contradiction, the probabilistic protocol must have nonzero probability for at least one entangled state.) Now, from [17] it follows that any complete product basis can be distinguished probabilistically [26]. Indeed in [17] it was shown that any separable superoperator can be performed by LOCC with some probability of success. However, measuring a complete product basis amounts to applying some separable superoperator. This ends the proof.

One can now try to see how effective the presented method is, when we deal with an incomplete set of orthogonal states. In that direction, let us now examine a case of indistinguishability of three orthogonal two-qubit states. This case has been solved in [5]. But we want to solve it by our method. As we would see, it leads to an interesting open question. Consider again therefore a four party state

$$|\chi\rangle = \frac{1}{\sqrt{3}} \sum_{i=1}^{3} |A_i\rangle_{AB} |B_i\rangle_{CD}$$

shared between Alice, Bob, Claire and Danny, to probe (by our method) the indistinguishability of the three orthogonal states $|A_i\rangle$ given by

$$\begin{aligned} |A_1\rangle &= a|00\rangle + b|11\rangle, \\ |A_2\rangle &= b|00\rangle - a|11\rangle, \\ |A_3\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \end{aligned}$$

where a and b are real (with $a^2 + b^2 = 1$) and the detectors $|B_i\rangle$ are the Bell states. Let us again suppose that the three orthogonal states $\{|A_i\rangle\}$ are distinguishable by LOCC even if only a single copy is provided. But this implies that Alice and Bob would be able to create the states $|B_i\rangle$ ($i = 1,2,3$) (each with probability 1/3) between Claire and Danny. Thus from the state $|\chi\rangle$, in the AC:BD cut, it would be possible to create the states $|B_i\rangle$ (i=1,2,3), each with probability 1/3, by LOCC only. According to the Jonathan-Plenio result [27] the process is impossible, if one of the squares of the Schmidt coefficients of ψ_{ABCD} across AC:BD cut is smaller than 1/2. We see that this is the case when a satisfies $.0252632 < a < .999681$. Thus the $|A_i\rangle$s ($i = 1,2,3$) are locally indistinguishable whenever a falls in the above range. However as shown recently by Walgate and Hardy [5] three two-qubit vectors can be distinuguished if only one of them is entangled [20]. Thus we should be able to show that the process of distinguishing by LOCC is impossible within the whole range $0 < a < 1$. We have tried with many different detectors, but the Bell states are most probably the optimal one. This intuition comes from the feeling that maximally entangled states would be the hardest to create. Therefore, change of detectors would possibly not produce the desired impossibility. We can however achieve it by putting probabilities:

$$p_1 = p_2 = 1/4, \quad p_3 = 1/2$$

instead of $p_i = 1/3$. For such probabilities we obtain that distinguishing between the states $|A_i\rangle$ leads to increasing some entanglement monotone in the whole range of parameter a.

Whether all (nonlocal) superoperators, which distinguish between *locally* indistinguishable states, would increase at least one LOCC monotone (by our scheme or otherwise) is an interesting open question. For example, it would be of interest to find out whether any superoperator which distinguishes between the states exhibiting nonlocality without entanglement [3] would increase some LOCC monotone or not. It is obvious that an initial product state across the AC:BD cut is useless for this case. Indeed, separable superoperators (which can distinguish vectors of a full product basis) cannot *create* entanglement: they cannot produce a non-product state out of a product one. Even PPT superoperators [29] (which can always distinguish vectors of an unextendible product basis [15]) can not change a product (hence PPT) state into a pure entangled (hence not PPT) state. Nevertheless it is not excluded that an initial entangled state (across the AC:BD cut) may detect nonlocality of such superoperators.

We are grateful to Charles Bennett for drawing our attention to the fact, that a complete set of orthogonal product states are always probabilistically distinguishable locally at the European Research Conference on Quantum Information in San Feliu de Guixols, Spain, March, 2002. The work is supported by the European Community under project EQUIP, Contract No. IST-11053-1999 and by the University of Gdańsk, Grant No. BW/5400-5-0236-2.

References

[1] The class of operations thay can perform is then called LOCC (local operations and classical communication) [2].

[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, Phys. Rev. A **54**, 2046 (1996) (quant-ph/9604024)

[3] C.H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, W.K. Wootters, Phys. Rev. A **59**,1070 (1999) (quant-ph/9804053)

[4] J. Walgate, A. Short, L. Hardy, V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000) (quant-ph/0007098)

[5] J. Walgate and L. Hardy, quant-ph/0202034

[6] V. Vedral, M.B. Plenio, M.A. Rippin and P.L. Knight, Phys. Rev. Lett. **78**, 2275 (1997) (quant-ph/9702027); M. B. Plenio and V. Vedral Phys. Rev. A **57**, 1619 (1998) (quant-ph/9707035)

[7] G. Vidal, J. Mod. Opt. **47**, 355 (2000) (quant-ph/9807077)

[8] M. Horodecki, Q. Comp. Inf. **1**, 7 (2001) (available at http://www.rinton.com/journals/qiconline.html)

[9] B.M. Terhal, D. Leung and D.P. DiVincenzo Phys. Rev. Lett. **86**, 5807 (2001) (quant-ph/0011042)

[10] S. Ghosh, G. Kar, A. Roy, A. Sen(De) and U. Sen, Phys. Rev. Lett. **87**, 277902 (2001) (quant-ph/0106148)

[11] M.A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999) (quant-ph/9811053)

[12] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999) (quant-ph/0011095)

[13] D. Jonathan and M.B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999) (quant-ph/9903054)

[14] Note that it is not possible to have a complete basis in a tensor product Hilbert space where all but *one* states are product. [The reason is the following [15]. Let $\{|\psi_i\rangle \otimes |\phi_i\rangle\}$ be a set of $d-1$ product states in a d -dimensional Hilbert space $H_A \otimes H_B$. Then $\Gamma = I - \sum_i^{d-1} |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$ must have positive partial transpose (PPT) [16], where I is the identity operator over $H_A \otimes H_B$. But Γ is a one-dimensional projector, which can be PPT if and only if it is a projector of a product state.] However for the purposes of the proof of our Proposition, we only need that the corresponding set of orthogonal states contains at least one entangled state.

[15] C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, B.M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999) (quant-ph/9808030)

[16] A. Peres, Phys. Rev. Lett. **77** 1413 (1996) (quant-ph/9604005)

[17] J.I. Cirac, W. Dür, B. Kraus and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001) (quant-ph/0007057)

[18] In the Vidal approach [7], entanglement is defined simply as a quantity that does not increase under LOCC (cf. [19]).

[19] D. Rohrlich and S. Popescu, Phys. Rev. A **56** R3319-R3321 (1997) (quant-ph/9610044)

[20] S. Ghosh, G. Kar, A. Roy, D. Sarkar, A. Sen(De) and U. Sen, Local indistinguishability of orthogonal pure states by using a bound on distillable entanglement, to appear in Phys. Rev. A (quant-ph/0111136)

[21] K. Życzkowski, P. Horodecki, A. Sanpera and M. Lewenstein Phys.Rev. A**58**, 883 (1998) (quant-ph/9804024); K. Życzkowski, Phys. Rev. A **60**, 3496 (1999) (quant-ph/9902050)

[22] J.A. Smolin, Phys. Rev. A **63** (2001) 032306 (quant-ph/0001001)

[23] Suppose $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$ are real d dimensional vectors. Then $x \prec y$ (x is majorized by y) if for each k in the range $1, \ldots, d$

$$\sum_j^k x_j^\downarrow \leq \sum_j^k y_j^\downarrow$$

where $x_j^\downarrow$ and $y_j^\downarrow$ are elements of the vectors x and y respectively with their entries set in decreasing order.

[24] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999) (quant-ph/9708015)

[25] Note that $|\phi\rangle^*$ is entangled whenever $|\phi\rangle$ is entangled.

[26] There is a direct, geometrical argument showing that a complete product basis is always probabilistically distinguishable [Charles H. Bennett, private communication].

[27] Actually in the considered case, all final states have the same λ_i, so that the Jonathan-Plenio criterion reduces to Nielsen's one [11].

[28] D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin and B.M. Terhal, quant-ph/9908070

[29] E.M. Rains, Phys. Rev. A **60**, 173 (1999) (quant-ph/9809078)